visioning in the cloud features blocks, and 2) an API-based trust model establishment and application provisioning in the cloud.

[0047] These features blocks of FIG. **3**B are described as follows with regards to an SSH-based trust model establishment and application provisioning in the cloud features blocks. In accordance with the exemplary embodiments of the invention as illustrated in FIG. **3**B there is at:

[0048] Feature Block **1**: Instance/Image Template;

[0049] An SSH public key is pre-configured in the instance image

[0050] An SSH public key is associated with the target App "A"

[0051] Feature Block **2**: Instance Start-Up (e.g. Bootstrapping)

[0052] Instance is started and IP Address is assigned.

[0053] Feature Block **3**: Instance Operation

[0054] 1. Agent may make API calls to cloud infrastructure service provider to look-up InstanceID, verify the instance/domain is allocated to the Cloud Service Account of the organization enterprise; it is noted that the deployment user may be required to be authenticated regarding the target cloud-based instance where the application instance will be deployed and bootstrapped. That target instance may not need an explicit validation per se since the target instance IP Address and instanceID (in the cloud) may be selected and validated by the corporate administrator (as part of the provisioning/deployment process.

[0055] 2. Authorized "Deployment user" (Agent) associated with App A makes SSH connection to the instance at the IP Address from Step#2.

[0056] 3. Instance is validated by the Agent as a result of login access.

[0057] 4. Agent injects the master key from Corporate Data Center to the instance

[0058] 5. Assign secrets (master key) as environment variables of the instance

[0059] 6. StarttheAppA

[0060] 7. App A reads the secret

[0061] 8. As an example once the Application instance has at run-time access to the master key, the App instance can potentially decrypt other dataset or datastore specific encryption keys to get eventual access to the target datasets and/or datastores.

[0062] 9. The master key (secret) is deleted from the environent (once the App A has consumed it)

[0063] 10. SSH public key is deleted and subsequently the deployment user (Agent) logs out/disconnect over SSH

[0064] Feature Block **4**: Instance Shutdown

[0065] As part of instance being terminated there is no clean up required (i.e., master key will also be deleted as part of the instance and corresponding App A being shutdown)

[0066] The feature blocks of FIG. **3**B are described as follows with regards to an API-based trust model establishment and application provisioning in the cloud. In accordance with the exemplary embodiments of the invention as illustrated in FIG. **3**C there is at:

[0067] Feature Block **1**: Instance/Image Template:

[0068] SSL client public key or API signing keys are preconfigured in the instance image to establish trust by the Deployment user (Agent) with the instance

[0069] Feature Block **2**: Instance Start-Up (e.g. Bootstrapping)

[0070] Instance is started and the App A is started

[0071] App A has specific API end-point, which is initialized (i.e., it is in listening mode)

[0072] Feature Block **3**: Instance Operation

[0073] API call invoked via API signing keys and server SSL or mutual SSL authentication using both server and client certificates.

[0074] SSL client certificate/public key or API signing keys must be removed from the instance once the injection of the master key is completed via the API call completion

[0075] Feature Block **4**: Instance Shutdown

[0076] As part of instance being terminated there is no clean up required (i.e., master key will also be deleted as part of the instance and corresponding App A being shutdown)

[0077] FIGS. **4**, **5**, **6**, and **7** illustrate for AWS as a nonlimiting example a production misuse/internal security map. In FIG. **4** there is illustrated a complete picture describing interactions between a cloud application provider and a legal authority, in this case the provider is referred to as Amazon®. FIGS. **5**, **6**, and **7** zoom in on various areas of the map as well as comments regarding issues associated with this interaction which the exemplary embodiments of the invention can address.

[0078] FIG. **8** illustrates a logic flow diagram of a nonlimiting operation of a method, and a result of execution of computer program instructions, in accordance with exemplary embodiments of this invention. As illustrated in step **8**A there is deploying, with a device of a private network, an application instance with an application web service in a cloud network; and as illustrated in step **8**B of FIG. **8** there is, based on the deploying, communicating with the application web service in the cloud network to establish a trust relationship with the application web service for the application instance.

[0079] In accordance with the exemplary embodiments of the invention as described in the paragraph above, the deployment script is defined in a machine image for the application instance.

[0080] In accordance with the exemplary embodiments of the invention as described in the paragraphs above, the machine image when started passes at least one of a username and password, or a security key to the application instance.

[0081] In accordance with the exemplary embodiments of the invention as described in the paragraphs above, the communicating comprises: connecting to the application image using the security key passed to the application instance; deploying a child certificate into the application image for the trusted relationship.

[0082] In accordance with the exemplary embodiments of the invention as described in the paragraphs above, there is after the connecting, assigning secrets read from environmental variables to the application instance for the trusted relationship, wherein the environmental variables are from a location controlled by the private network.

[0083] In accordance with the exemplary embodiments of the invention as described in the paragraphs above, the machine image, when started for the application instance, loads a deployment agent to connect back to the private network.